Preparar pfSense para el aula

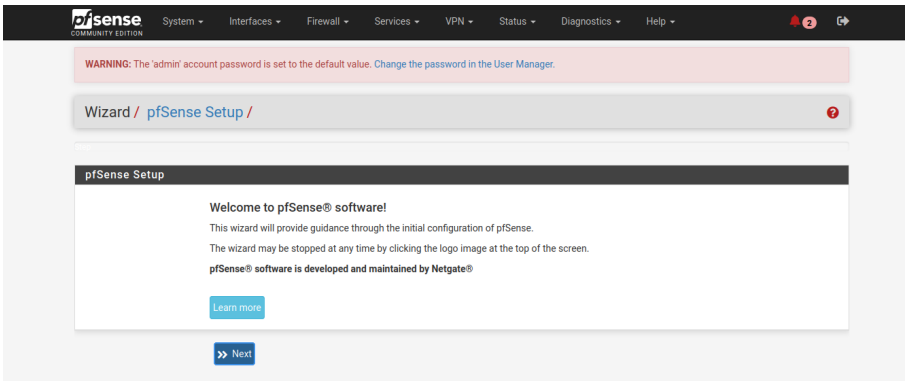
Arcadio Ortega Reinoso

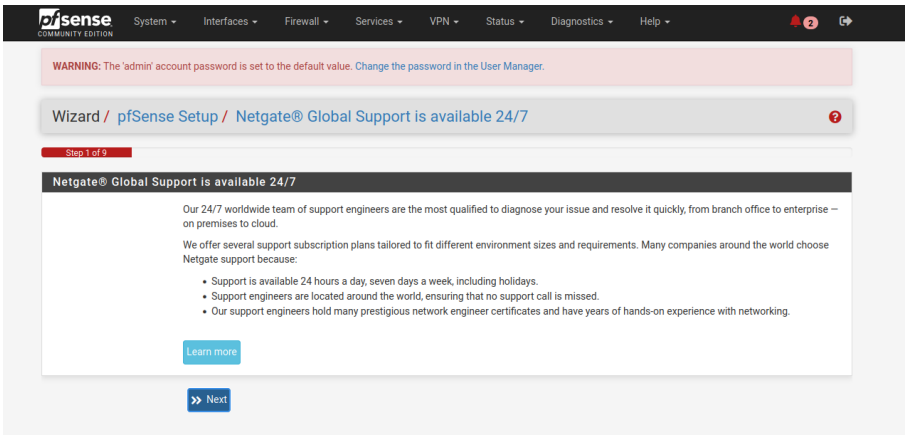
Este documento está bajo licencia:

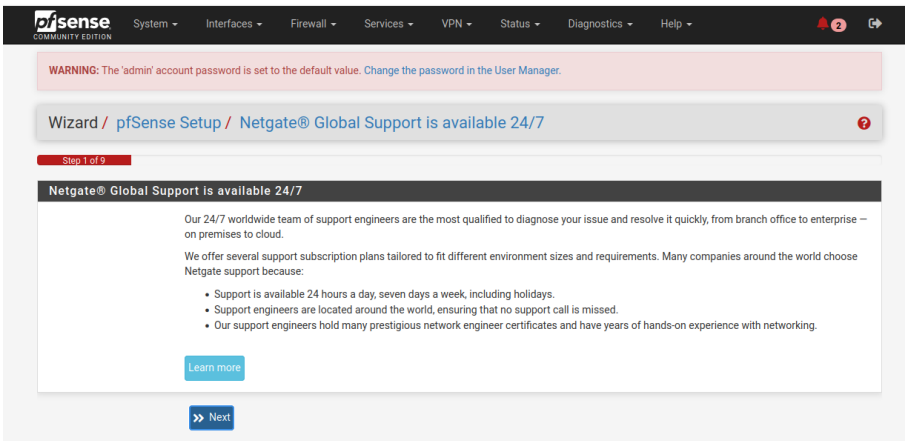
Atribución – No Comercial – Compartir Igual (CC BY-NC-SA 4.0)
Puedes compartir, copiar, redistribuir y adaptar esta obra con fines no comerciales,
siempre que cites al autor y mantengas esta misma licencia para cualquier derivado.

pfsense

Instalación

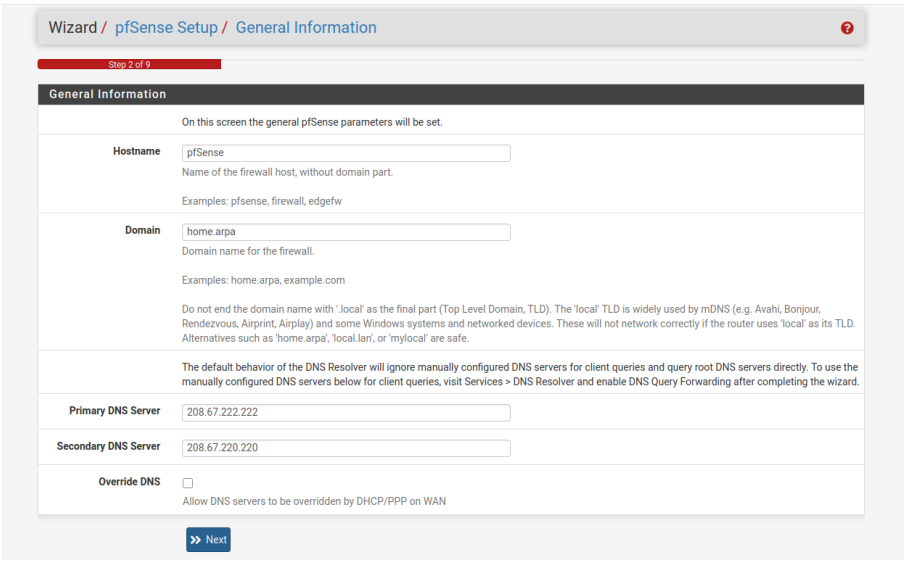




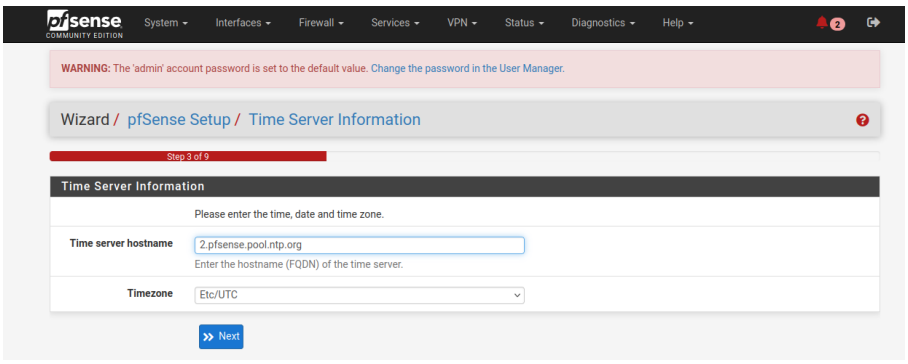


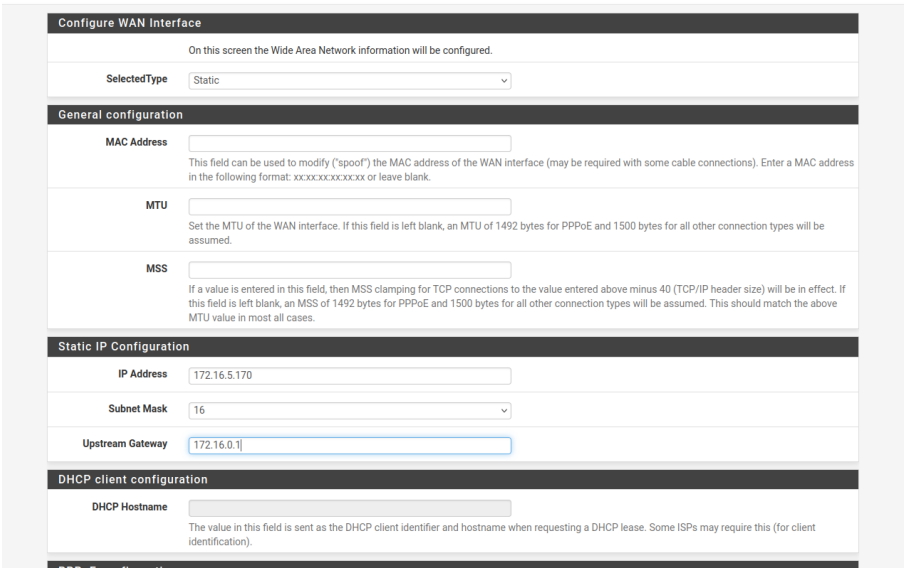
Configuramos los datos: Vampos a utilizar en primera medida como servidores de DNS los de **openDNS** para "familias"

O el de nuestro IPA server si lo estamos usando y desde allí se trabajará con los forwards de openDNS por ejemplo.



Respecto al servidor de NTP podemos usar el que hemos dado de alta en nuestro IPA server (Si fuiera el caso)





"Block private networks" (bloquear redes privadas — hace referencia a RFC1918)

Esta opción impide que las direcciones IP privadas, definidas por la RFC1918, accedan a la interfaz en la que se activa esta opción. Las redes privadas RFC1918 son:

- 10.0.0.0/8
- 172.16.0.0/12

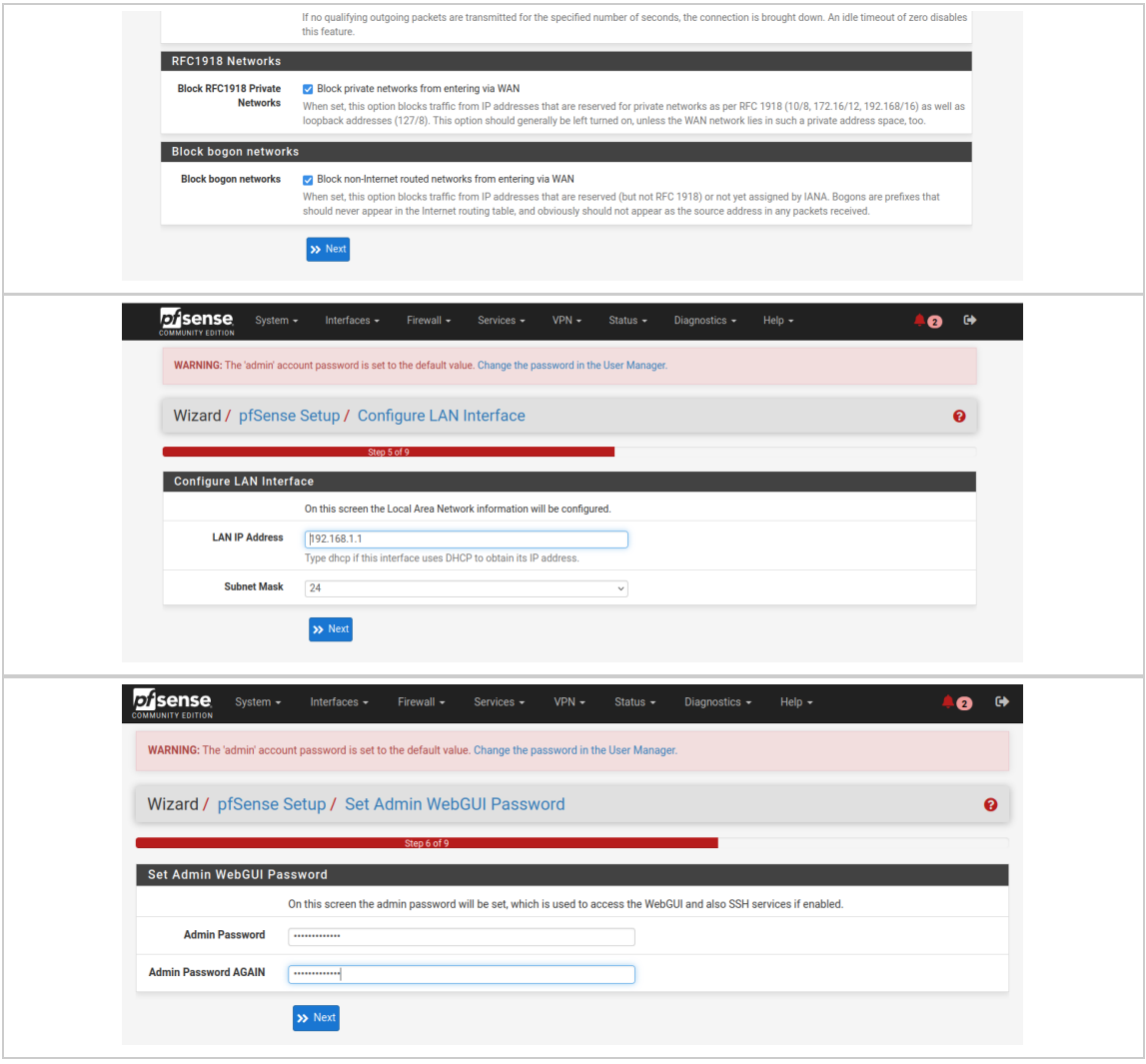
- 192.168.0.0/16

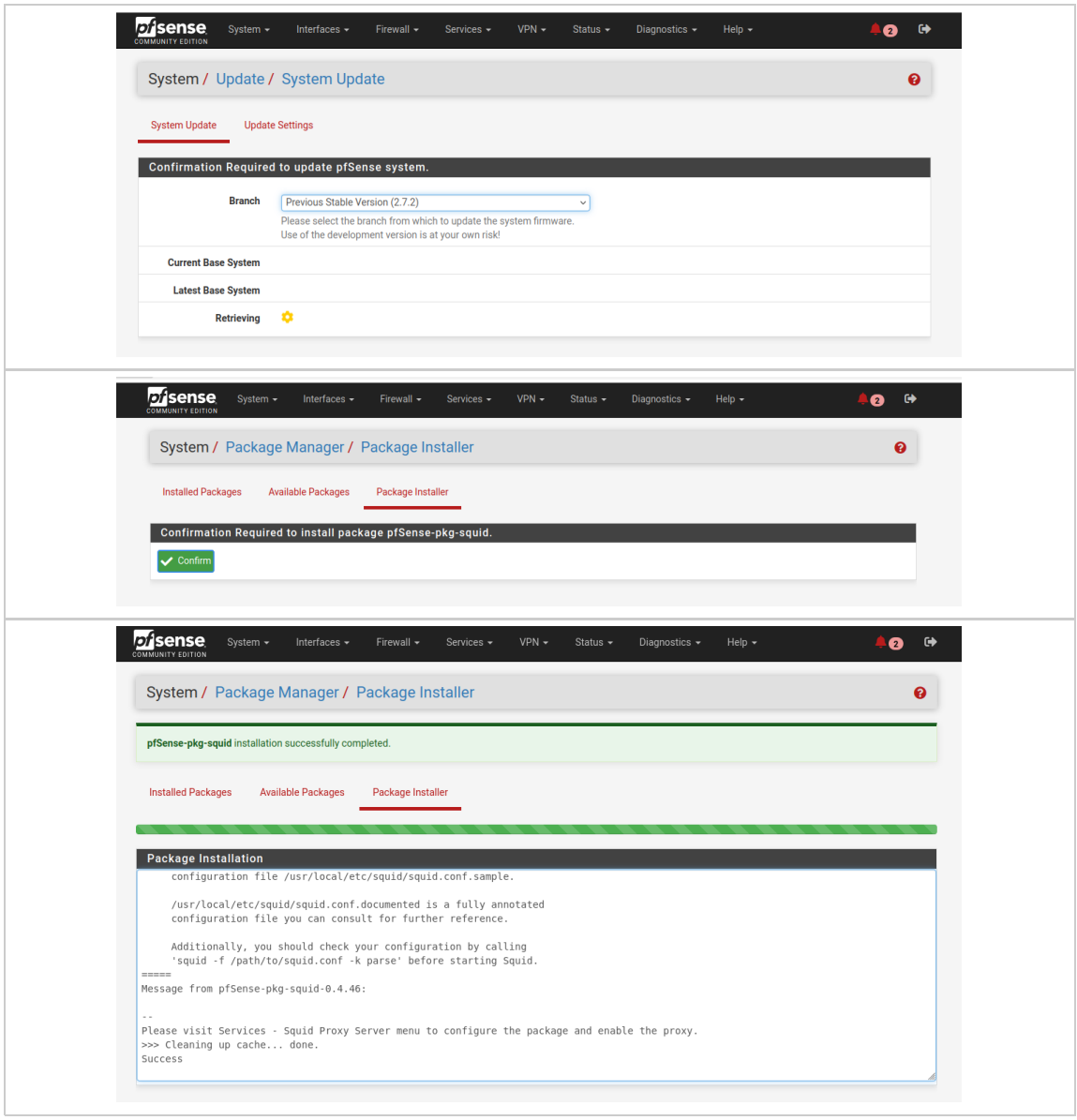
pfSense debería bloquear cualquier tráfico que provenga de esas IPs en la WAN. redes privadas en la WAN usualmente indica una configuración incorrecta o un posible intento de ataque.

"Block bogon networks" (bloquear redes "bogon")

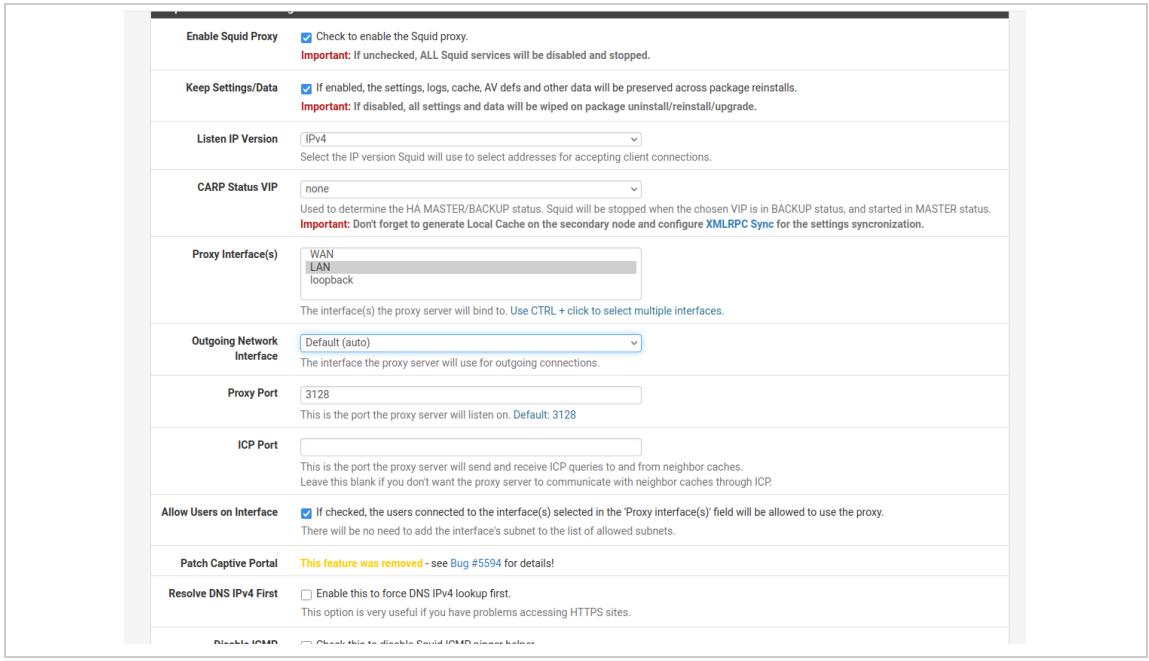
Las redes bogon son direcciones IP que no deberían estar enrutadas públicamente en Internet. Incluyen:

- Espacios IP no asignados por IANA (como subredes nuevas aún no delegadas)
- IPs reservadas para uso futuro o especial
- Algunas direcciones privadas o experimentales adicionales (aparte de RFC1918)

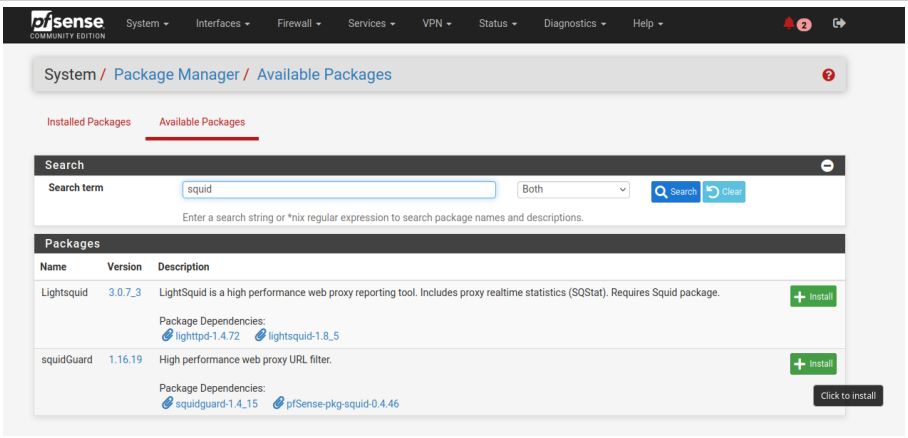


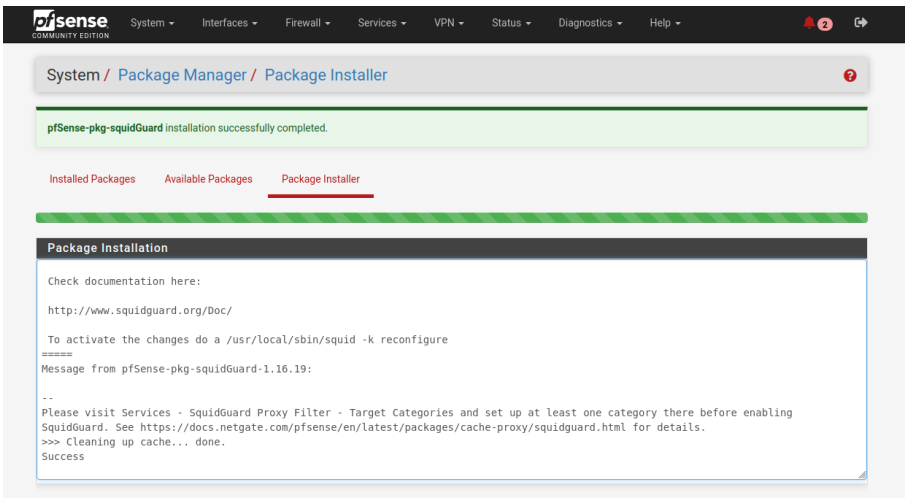


Squid proxy

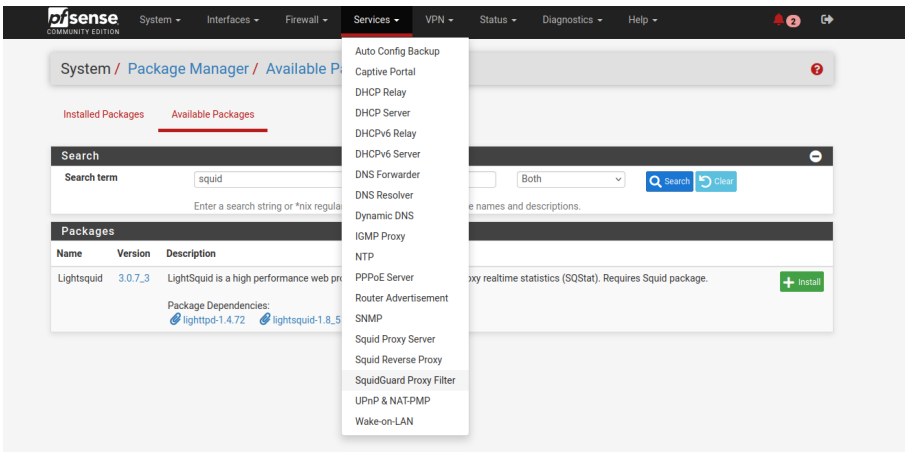


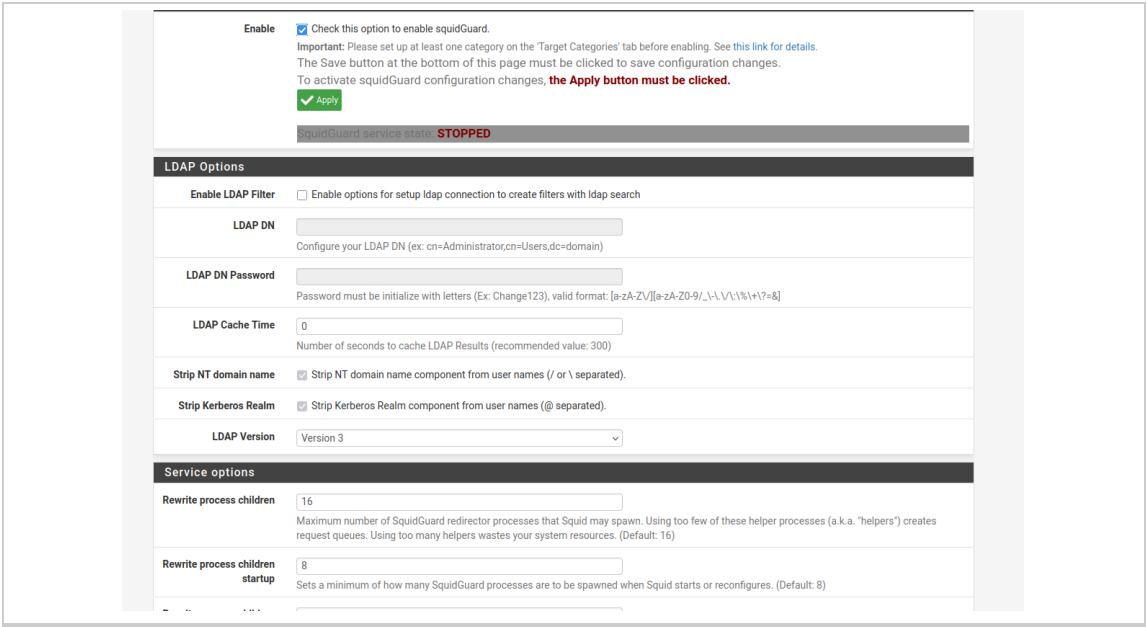
Squid Guard

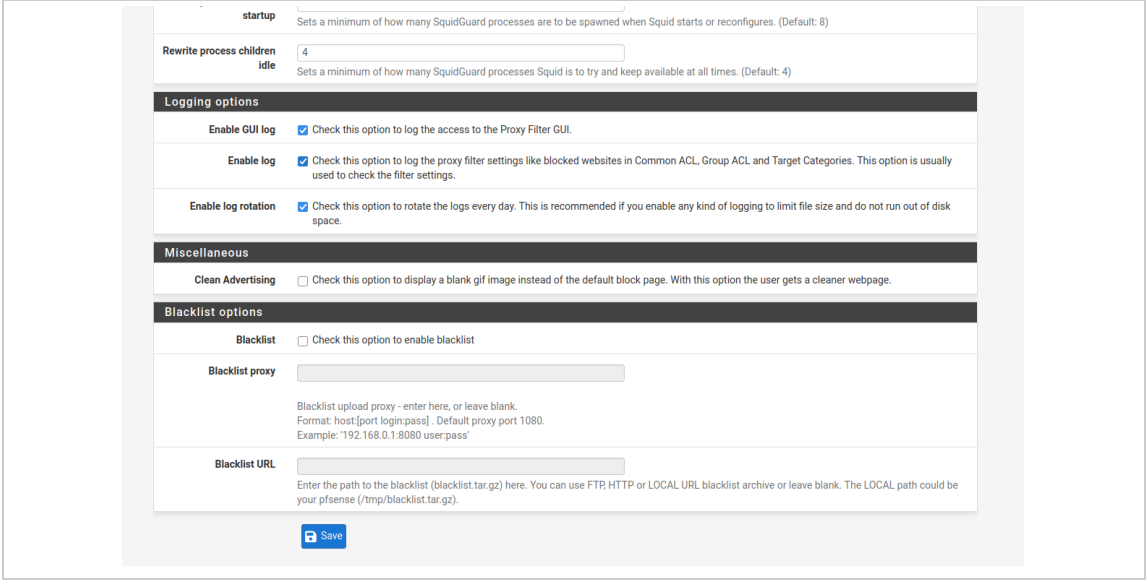


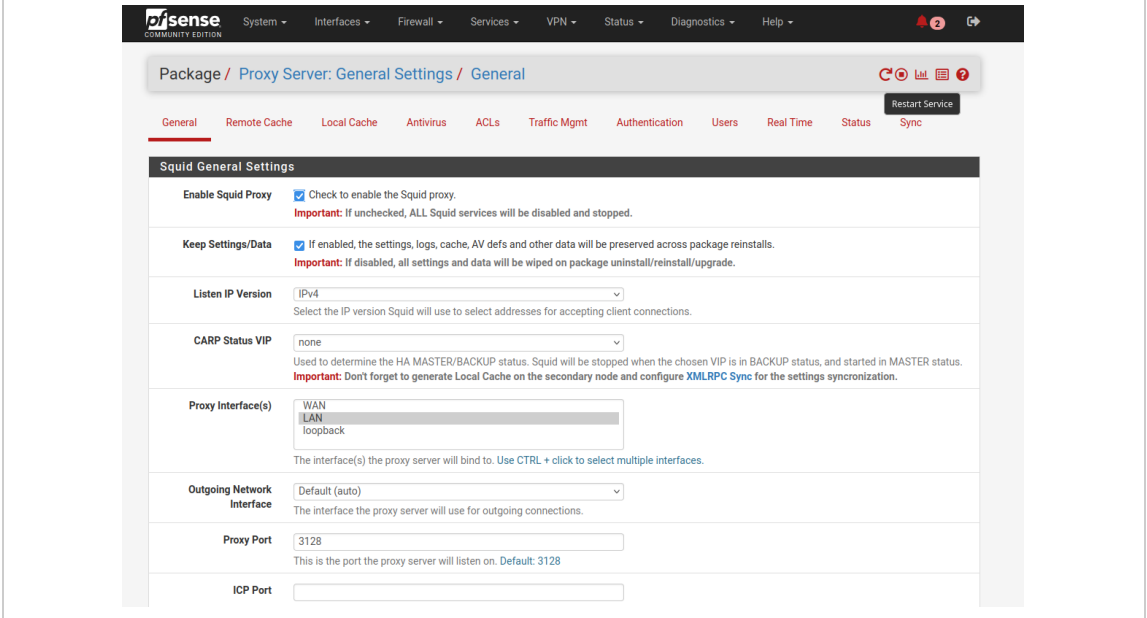


Squid proxy filter

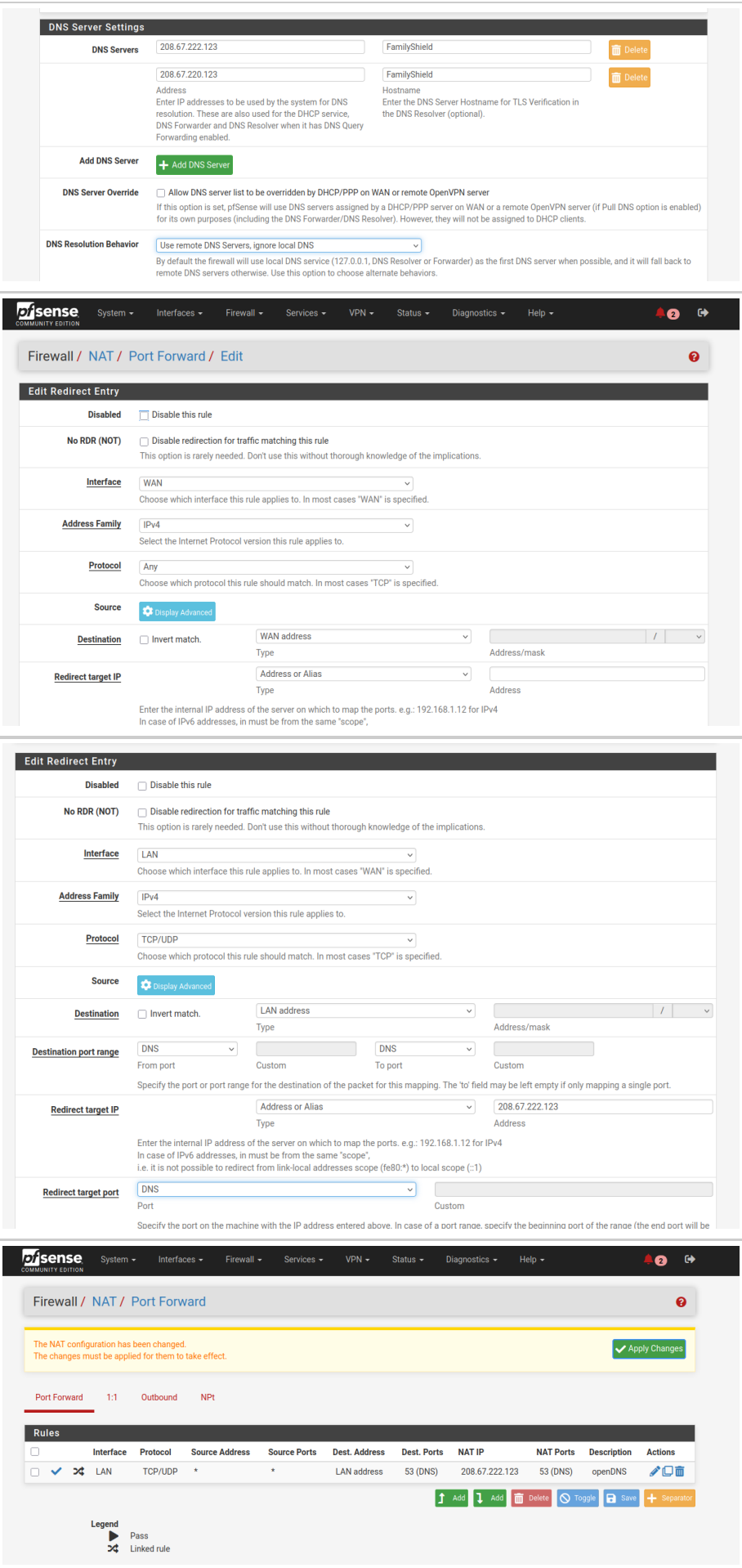



Enable
Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, the Apply button must be clicked.
Apply
SquidGuard service state: STOPPED
LDAP Options
Enable LDAP Filter
Enable options for setup ldap connection to create filters with ldap search
LDAP DN
Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)
LDAP DN Password
Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z\][a-zA-Z0-9/_\-\.\/\:\%\+\?=&]
LDAP Cache Time
0
Number of seconds to cache LDAP Results (recommended value: 300)
Strip NT domain name
Strip NT domain name component from user names (/ or \ separated).
Strip Kerberos Realm
Strip Kerberos Realm component from user names (@ separated).
LDAP Version
Version 3
Service options
Rewrite process children
16
Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)
Rewrite process children startup
8
Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)

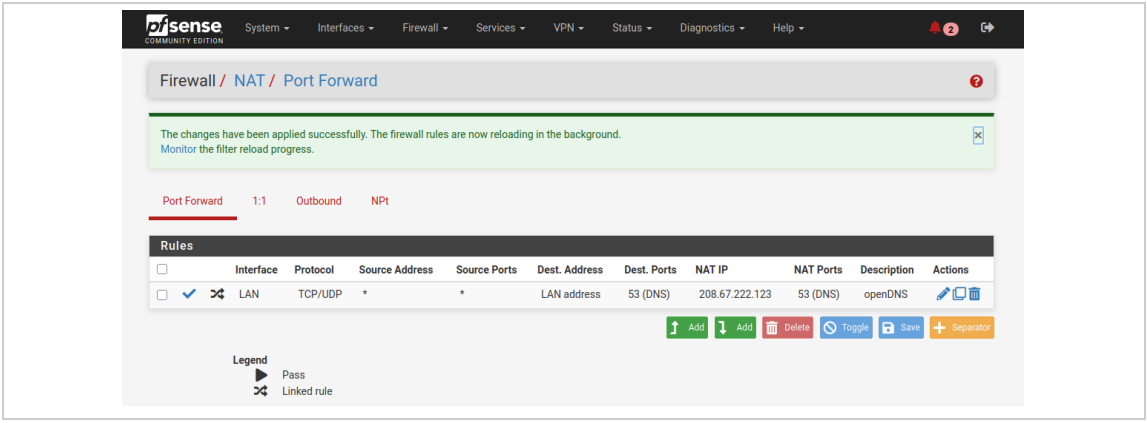

startup
Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)
Rewrite process children idle
4
Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)
Logging options
Enable GUI log
Check this option to log the access to the Proxy Filter GUI.
Enable log
Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation
Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.
Miscellaneous
Clean Advertising
Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.
Blacklist options
Blacklist
Check this option to enable blacklist
Blacklist proxy
Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'
Blacklist URL
Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).
Save


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy Server: General Settings / General
Restart Service
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
Squid General Settings
Enable Squid Proxy
Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data
If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version
IPv4
Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP
none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings syncronization.
Proxy Interface(s)
WAN
LAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface
Default (auto)
The interface the proxy server will use for outgoing connections.
Proxy Port
3128
This is the port the proxy server will listen on. Default: 3128
ICP Port

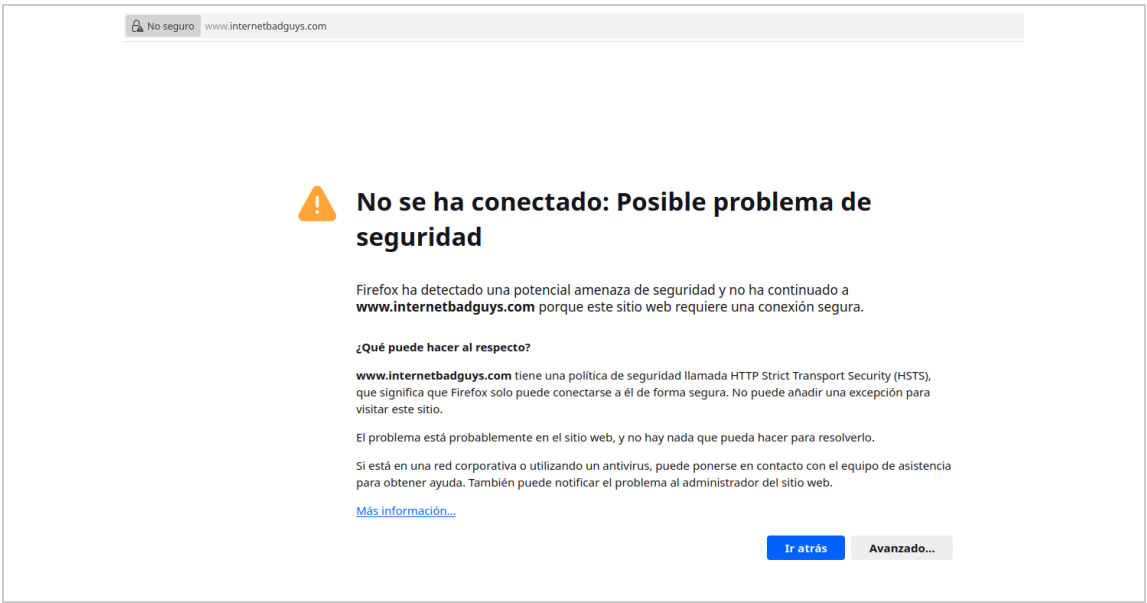
DNS setting

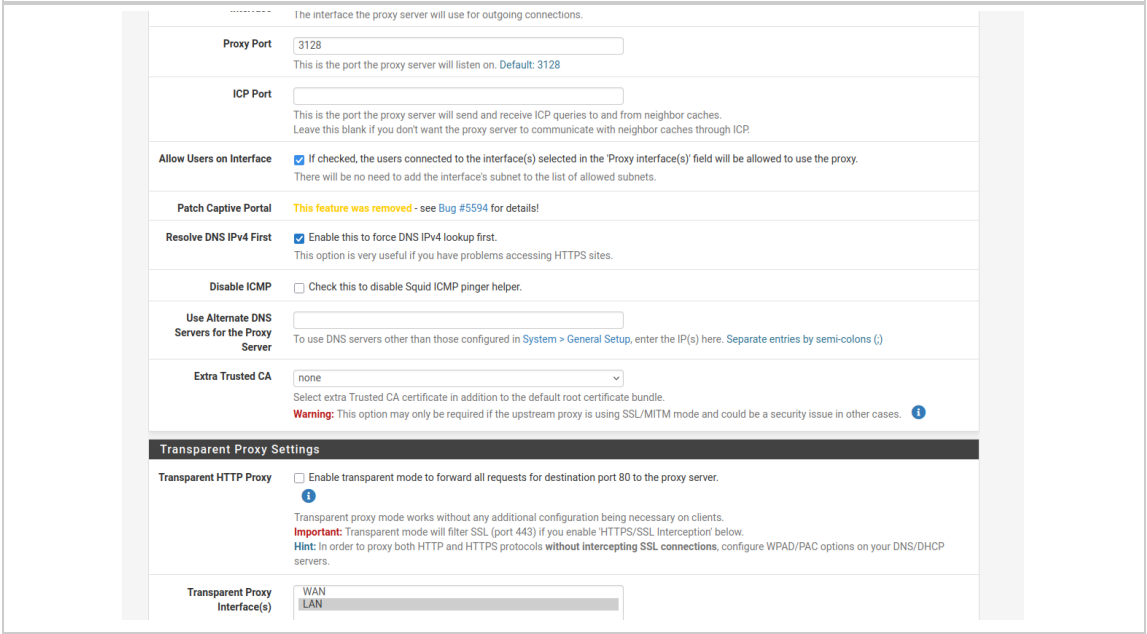


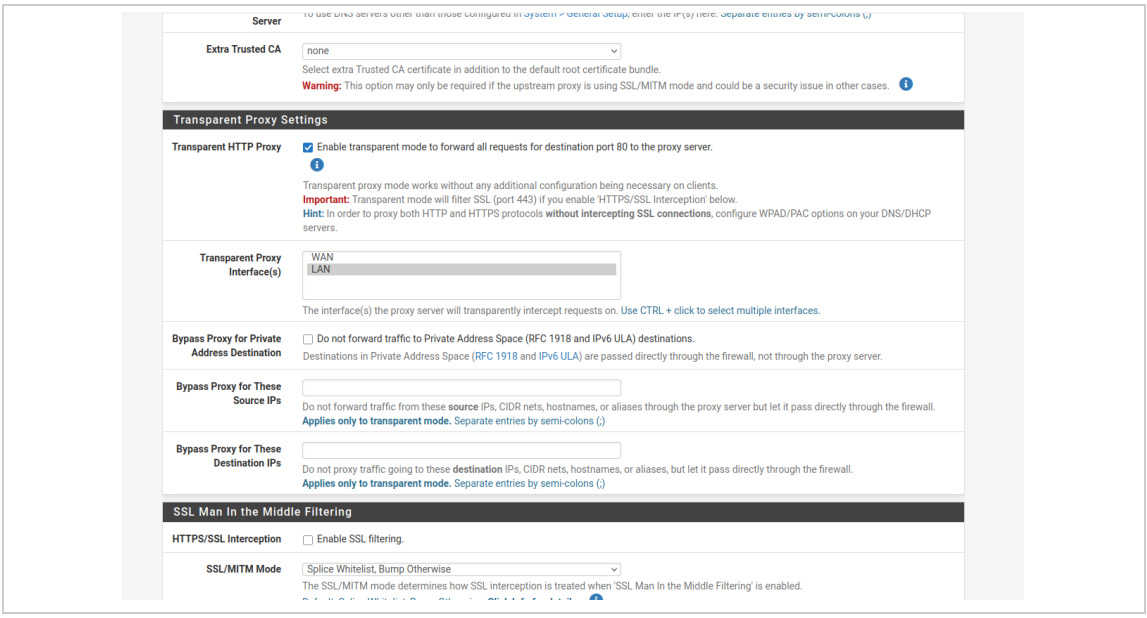
Cada vez que cambiemos algo tenemos que aplicar los cambios.



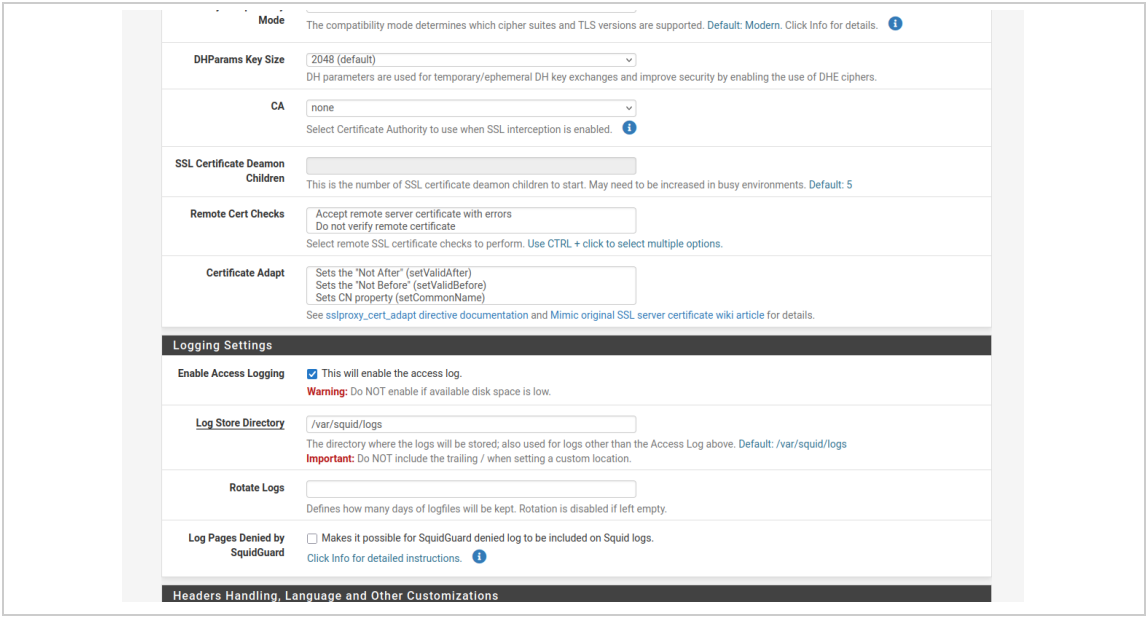
Realizamos la prueba para verificar que openDNS se está aplicando correctamente:



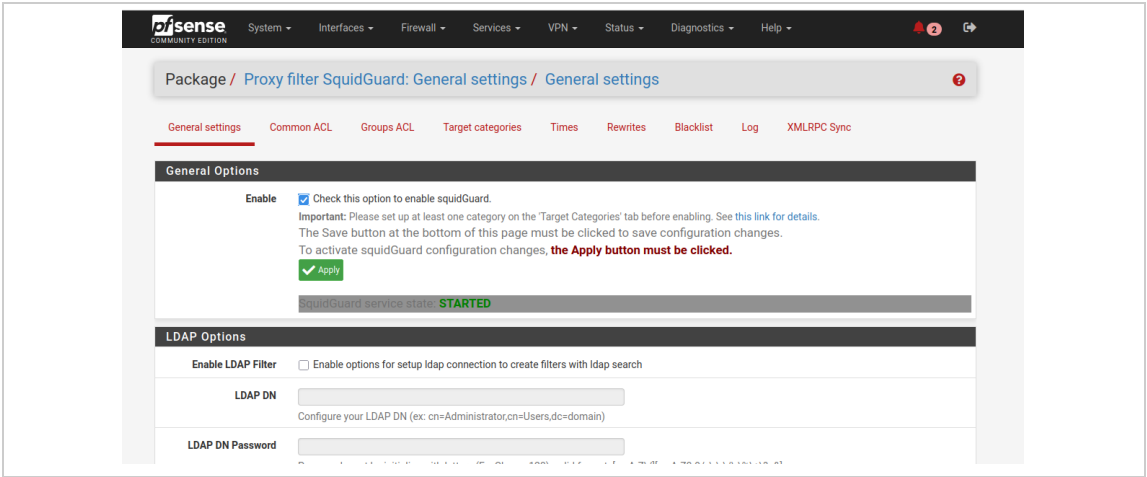




Activamos el sistema de Log para este caso.

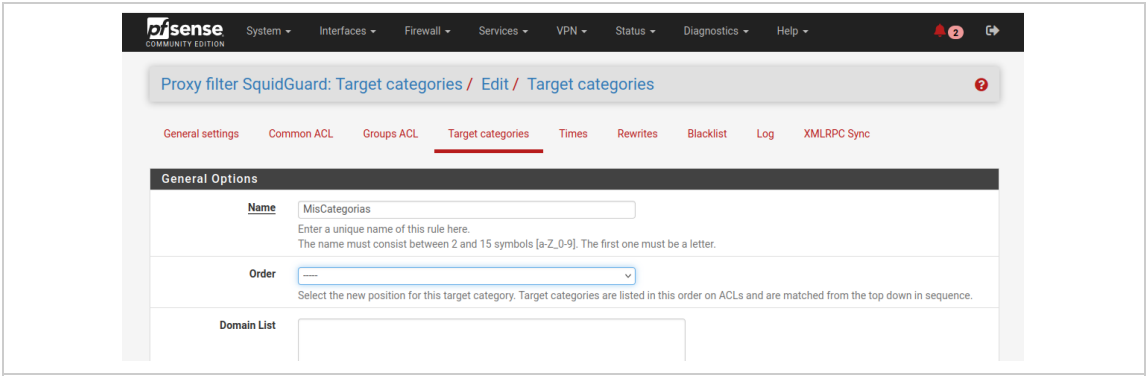


Aplicamos los cambios

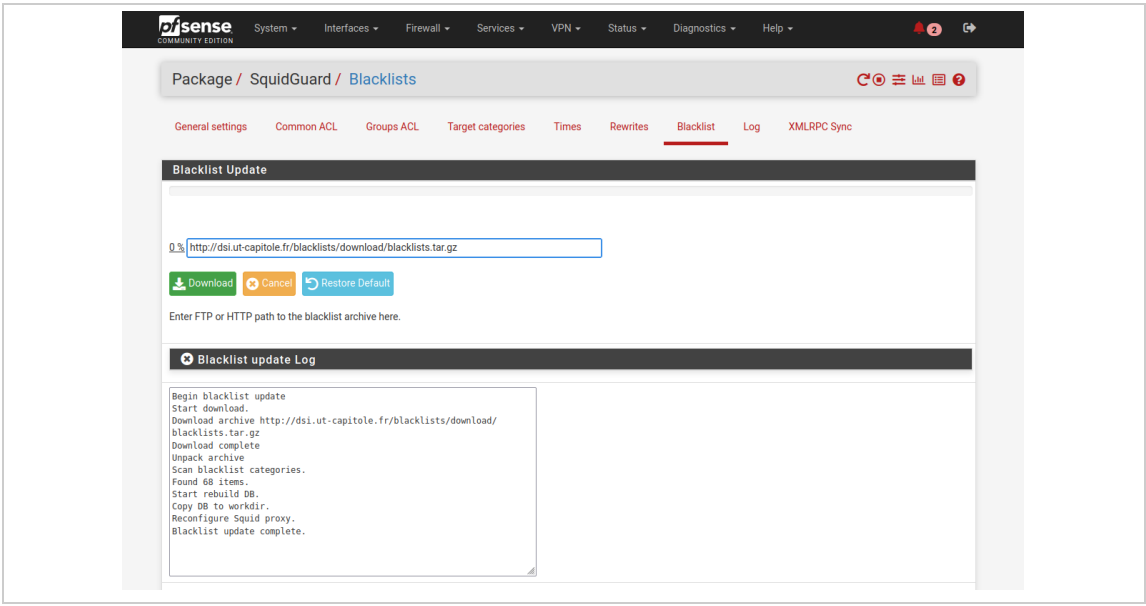


Blacklist

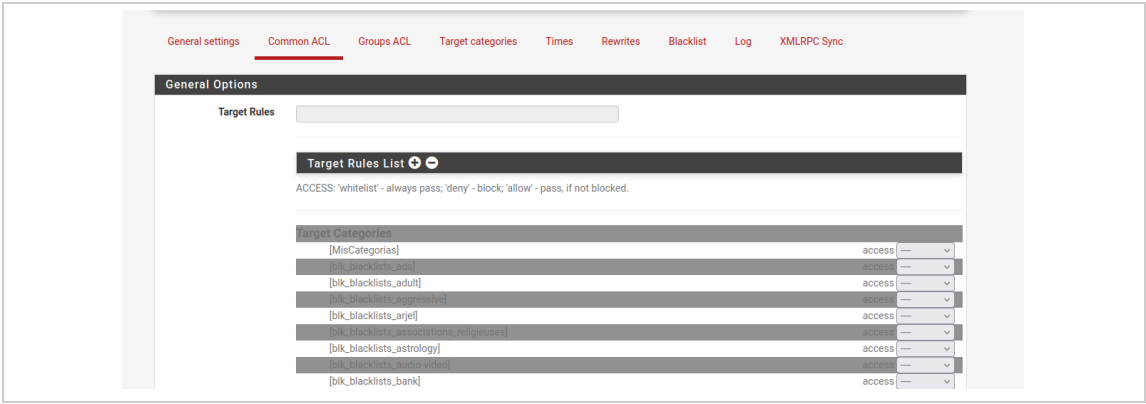
Lo primero es crear manualmente una categoría que es la que va a recoger todos nuestros datos



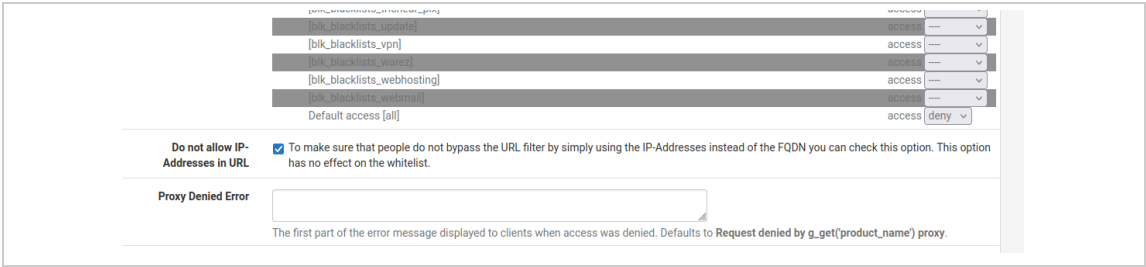
Aplicamos nuestra lista negra



Seleccionamos los grupos de nuestra lista negra que vamos a aceptaro o denegar o a tratar como lista blanca:



Para que no nos salten es importante negar el uso de direcciones ip de manera directa:

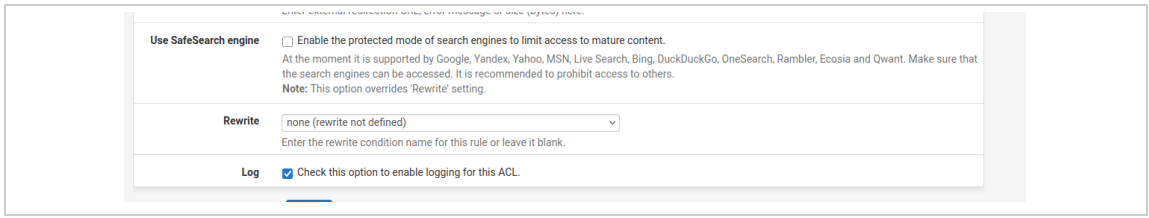


Permitimos que existan logs de lo que estamos haciendo

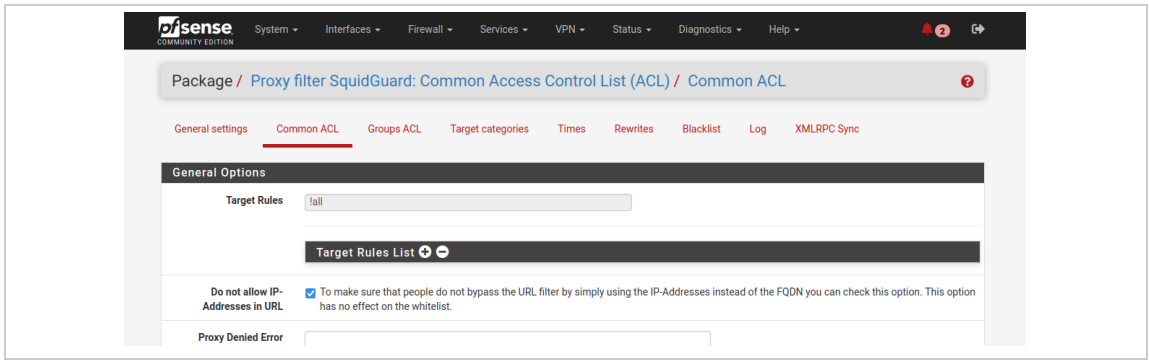
Además podemos usar: La opción **Use SafeSearch** fuerza a los motores de búsqueda compatibles a activar automáticamente su modo de búsqueda segura, incluso si el usuario no lo ha activado manualmente.

Esto significa que se bloquean o filtran resultados que contengan contenido explícito, como:

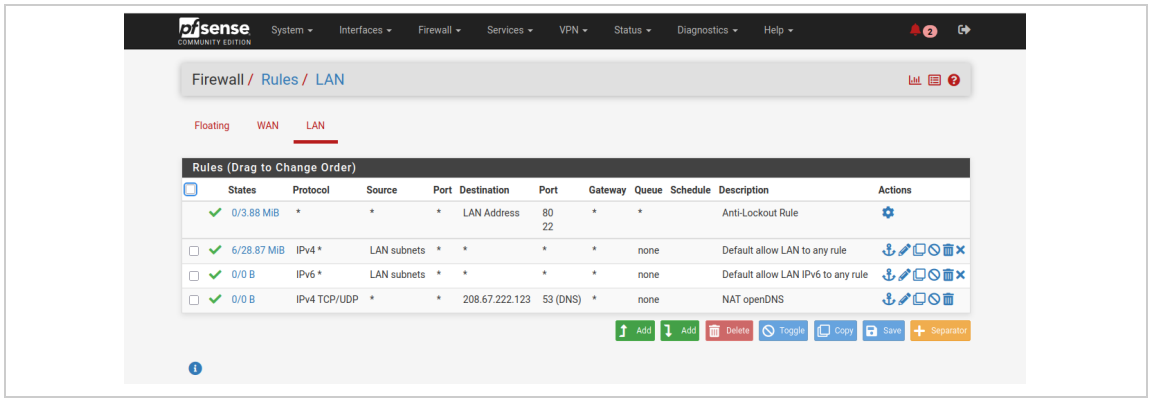
- Pornografía
- Imágenes de violencia
- Lenguaje explícito
- Resultados NSFW



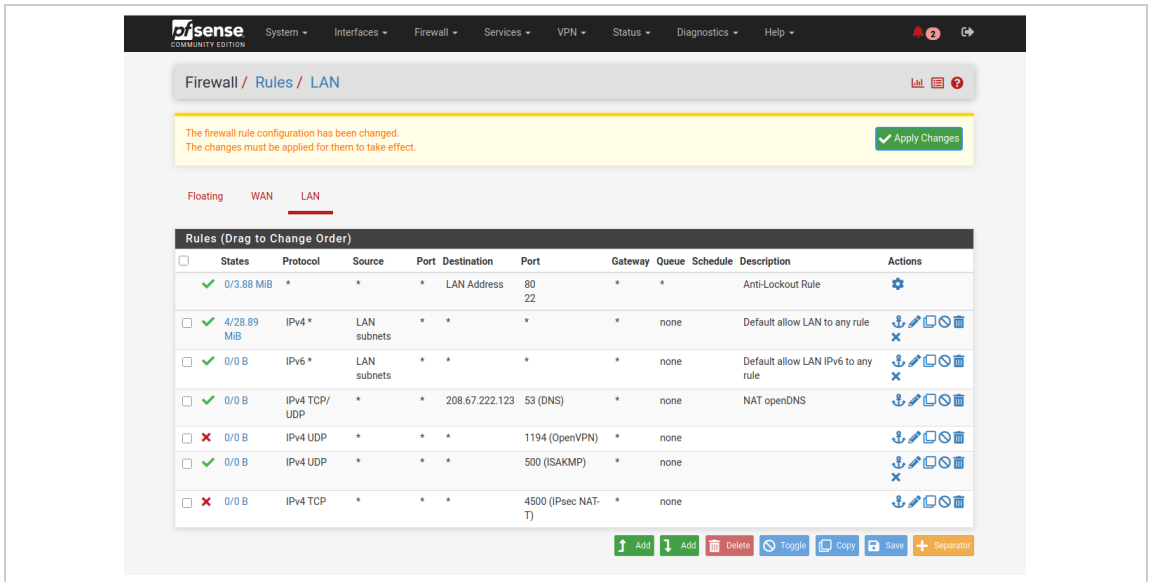
Ejemplo del resultado de nuestro target:



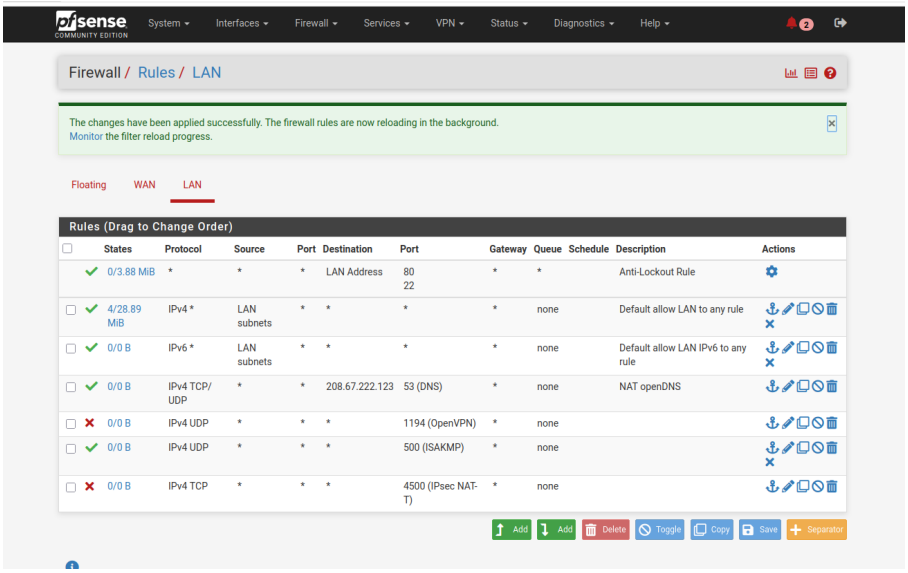
Firewall. Reglas



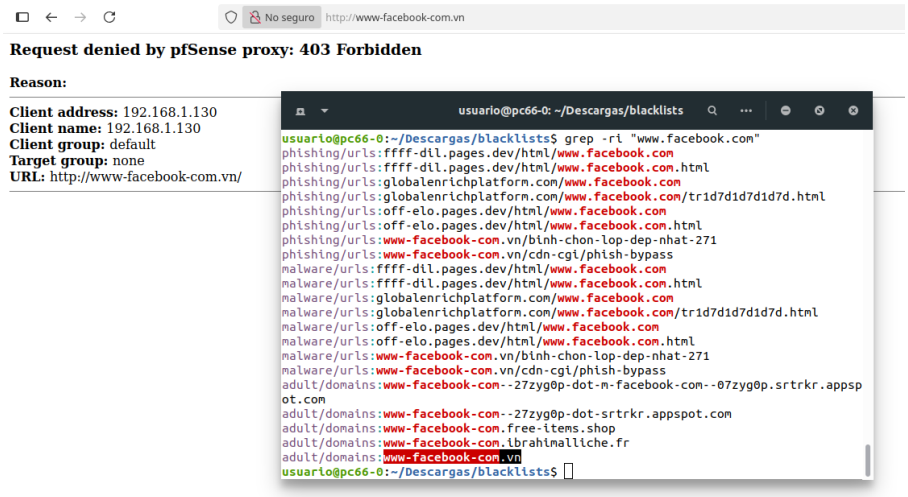
Podemos limitar el uso de VPNs por ejemplo:



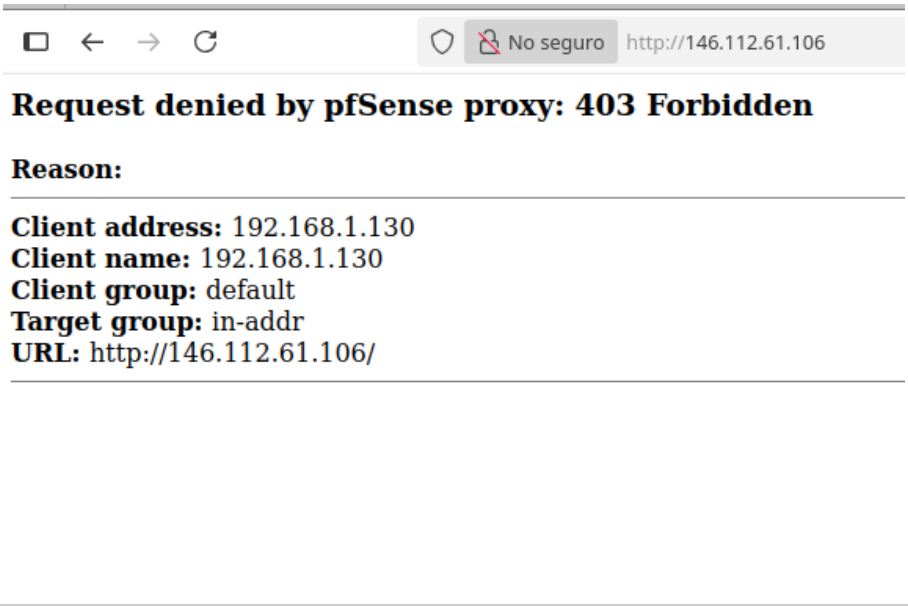
Cada vez que se haga un cambio hay que aplicarlo

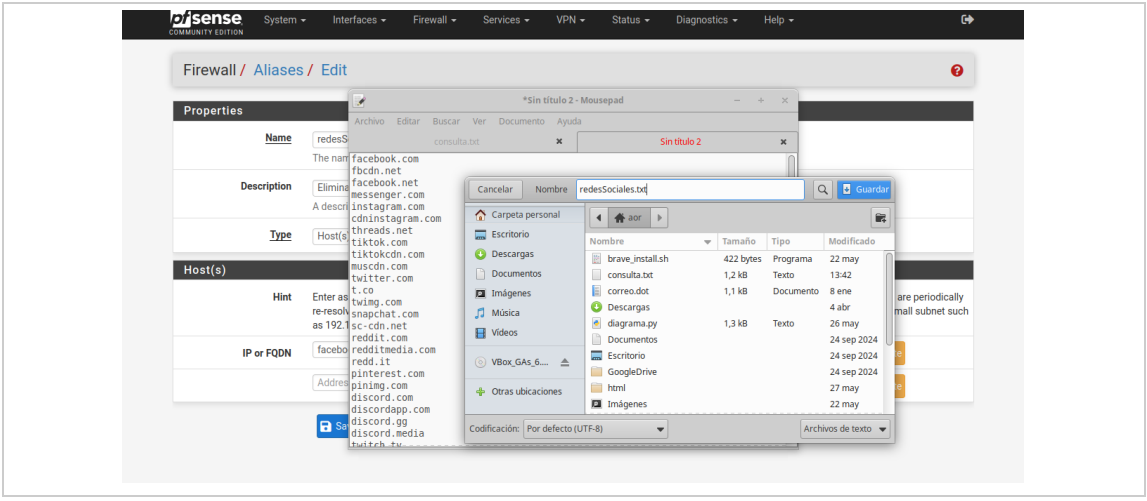


Podemos buscar una entrada de nuestra lista negra y ver si se está restringiendo su acceso:



De la misma manera si damos directamente una dirección ip





Notas

Para el teclado en español: Añadir una primera línea a /root/.profile con lo siguiente:

```
/usr/sbin/kbdcontrol -l /usr/share/syscons/keymaps/spanish.iso.kbd
```

Enlaces de interés

- ut-capitole blacklist